HEALTH AFFAIRS

TRICARE
Management
Activity

Oversight and Compliance

TMA Privacy Office

This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.

Agenda

- Oversight
- Compliance Assurance

Training Objectives

- Upon completion of this lesson, you will be able to:
  - Describe the reasons for Oversight
  - List methodologies for Compliance Assurance

Oversight

Be Vigilant **–**

Crede sed Certum Proba

“Trust but prove a thing certain”

Oversight

Objectives

- Upon completion of this module, you will be able to:
  - Describe the requirements and reasons for Oversight
  - List existing oversight responsibilities
  - Explain oversight in the joint organizational structure of the MHS

Why Do We Need Oversight? (1 of 2)

- Just look at headlines in in the news:
  - *Bank of America Lost Computer Tapes*
  - *County Worker in West Palm Beach, Florida Sends E-Mail With Residents AIDS and HIV Status*
  - *ChoicePoint Sold Personal Information To IdentityThieves*
  - *Gartner Group Estimates More Than 9.4 million U.S. Adults Victimized By Identity Theft*

Why Do We Need Oversight? (2 of 2)

- Headlines (cont.)
  - *Federal Trade Commission (FTC) Initiates Enforcement Action Against Two Mortgage Companies For Lax Data Security*
  - *DoD Scores "D" on the 2004 Federal Computer Security Report Card*

Oversight

What is Oversight?

- An independent evaluation of programs and operations to determine whether
  - Applicable laws, regulations, and policies are followed
  - Management/Internal control systems are adequate
  - Information is reliable, accurate, and available
  - Resources are safeguarded and managed economically and efficiently
  - Desired program results are achieved

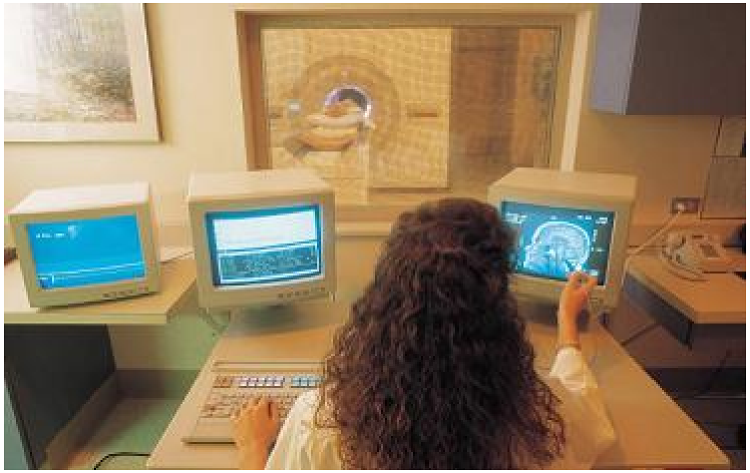
Multiple Requirements for Oversight (1 of 4)

- Department of Defense
  - Extensive requirements for the use, access and sharing of different classifications of information and the management practices for information systems
    - Information Assurance
    - Classification of Data
    - Physical Security
    - Personnel Clearances
  - Difficulties lie in trying to tailor these requirements to medical information in general and PHI in particular

Oversight

Multiple Requirements (2 of 4)

- Health care organizations have many overlapping requirements
  - Must know all of the laws that apply to its data maintenance and transmission
  - Utilize the same strategy for information privacy and security regardless of if the requirement derives from HIPAA, GLBA, Sarbanes-Oxley, state or DoD



Oversight

Multiple Requirements (3 of 4)

Examples of overlapping requirements from the HIPAA Privacy and Security Rules

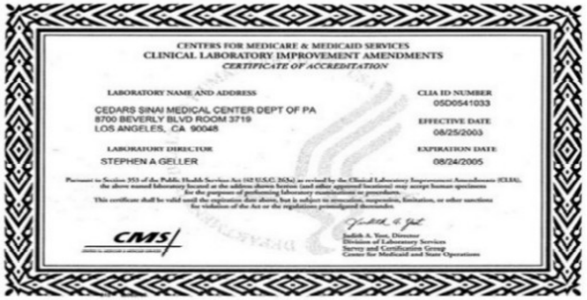
- Internal Audits
- Logical access controls
- Incident procedures
- Security / privacy management
- Sanctioning
- Training

- Assigned responsibility – HIPAA officers
- Physical access controls
- Business Associate Agreements
- Authorization controls
- Personnel Security

Oversight

Multiple Requirements (4 of 4)

- Civil Accreditation Requirements
  - Hospitals
    - Joint Commission on the Accreditation of Healthcare Organizations (JCAHO)



CENTERS FOR MEDICARE & MEDICAID SERVICES
CLINICAL LABORATORY IMPROVEMENT AMENDMENTS
CERTIFICATE OF ACCREDITATION

LABORATORY NAME AND ADDRESS
CEDARS SINAI MEDICAL CENTER DEPT OF PA
8700 BEVERLY BLVD ROOM 3719
LOS ANGELES, CA 90048

LABORATORY DIRECTOR
STEPHEN A GELLER

CLIA ID NUMBER
05D0541033

EFFECTIVE DATE
08/25/2003

EXPIRATION DATE
08/24/2005

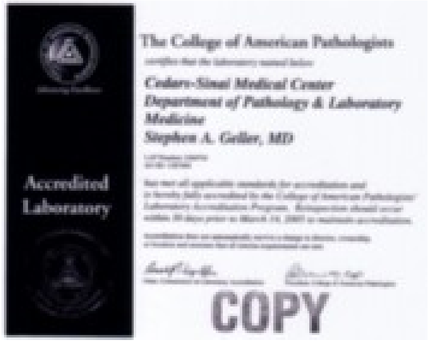
Pursuant to Section 353 of the Public Health Service Act (42 U.S.C. 263a) as revised by the Clinical Laboratory Improvement Amendments (CLIA), the above named laboratory located at the address shown hereon (and other approved locations) may accept human specimens for the purposes of performing laboratory examinations or procedures.

This certificate shall be valid until the expiration date above, but is subject to revocation, suspension, limitation, or other sanctions for violation of the Act or the regulations promulgated thereunder.

CMS

Judith A. Yost, Director
Division of Laboratory Services
Survey and Certification Group
Center for Medicaid and State Operations

  - Laboratories
    - Clinical Laboratory Improvement Act (CLIA) of 1967
    - College of American Pathologists (CAP)
  - Radiology
    - American College of Radiology (ACR)



Accredited Laboratory

The College of American Pathologists
certifies that the laboratory named below

Cedars-Sinai Medical Center
Department of Pathology & Laboratory Medicine
Stephen A. Geller, MD

[illegible]

has met all applicable standards for accreditation and is hereby fully accredited by the College of American Pathologists' Laboratory Accreditation Program. Reinspection should occur within 30 days prior to March 31, 2005 to maintain accreditation.

[illegible]

COPY

Oversight

Tri-Service Organization (1 of 2)

- MHS is a complex organization
  - Unique in government as a large medical component to an organization with a non-medical mission
  - Has 3 distinct branches of Services and the Coast Guard with individual rules, requirements and ways of doing business
  - Uniformed staff belong to the “line” while the funding and the medical policies are set by Health Affairs
- Core mission of the MHS remains the same across all components
  - *to provide medical care to our beneficiaries*!

Oversight

Tri-Service Organization (2 of 2)

- MHS is a joint command….
  - How can the Services ensure that the health data of their patients is adequately protected when patients are able to be seen at multiple facilities in the TRICARE system?
  - How can TRICARE, as the health plan, provide an accounting of disclosures for a patient if facilities maintain separate disclosure accounting systems?
  - How will any one Service be able to provide oversight of IT systems that interconnect across Services?
- …..Oversight is a joint responsibility

Summary

- You should now be able to:
  - Describe the reasons for Oversight
  - List existing oversight responsibilities
  - Explain oversight in the joint organizational structure of the MHS

Compliance Assurance

Compliance Assurance

Objectives

- Upon completion of this module, you will be able to:
  - List methodologies for Compliance Assurance
  - Describe current and proposed reporting requirements for HIPAA compliance
  - List the tools and resources available for oversight activities

Compliance Assurance Approach (1 of 3)

- Compliance Assurance - **Monitoring and reviewing** performance in areas of compliance risk to ensure
  - Established policies and procedures are being followed
  - Policies and procedures are effective
  - MHS HIPAA data is accurate and reliable

Compliance Assurance Approach (2 of 3)

- Methodologies for Compliance Assurance
  - Reports that provide information on compliance within organizations and across the enterprise
  - Metrics to gauge compliance performance and monitor the progress of HIPAA privacy and security programs

Compliance Assurance Approach (3 of 3)

- Methodologies for Compliance Assurance (cont.)
  - Program Reviews to ensure that information being reported on HIPAA compliance is accurate and complete
  - POA&M used to identify and monitor privacy and security-related programmatic and system-level weaknesses
  - Metrics to demonstrate the maturity of the organization’s HIPAA programs

Compliance Assurance

Current Reporting Requirements

- Monthly reports for HIPAA security implementation (December 2004 – TBD)
  - Data elements reported include:
    - Total number of facilities being reported
    - Total number of facilities that have completed the baseline security analysis using HIPAA BASICS^{TM}
    - Total number of facilities that have completed their risk assessments
    - Using HIPAA BASICS^{TM}, average compliance rate of all facilities
- Monthly reports for HIPAA Privacy and Security Training
  - Provided and recorded in LMS
- Quarterly updates to Deputy Surgeons General

Compliance Assurance

Proposed Reporting Requirements (1 of 3)

- Disclosures and Complaints
  - Monthly reports
  - Need several months of data to see stability in the metrics
- HIPAA Security Incidents
  - Draft of Incident Response Plan has stratified reporting
    - Immediate reporting of security incident involving ePHI
    - Monthly reporting of other data points for trend analysis

Compliance Assurance

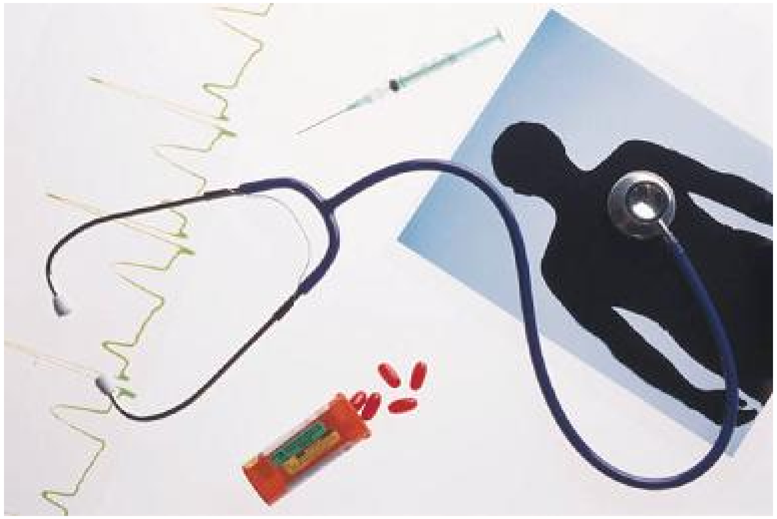
Proposed Reporting Requirements (2 of 3)

- Reports will be at multiple levels of the organization
  - TRICARE Health Plan (MHS)
    - Includes TMA, Army, Navy, Air Force, and the Coast Guard
    - Results will be provided to ASD(HA)
  - Service Medical Components/TMA
    - Included entities are at the discretion of the Services and TMA management
    - Results of the reports to be provided to the MHS on a periodic basis or as requested
  - Military Treatment Facilities
    - Includes clinics and satellite facilities

Compliance Assurance

Proposed Reporting Requirements (3 of 3)

- Recommendations for reports at the Military Treatment Facility level
  - Training Reports
  - Compliance Reports
  - Disclosure tracking



Compliance Assurance

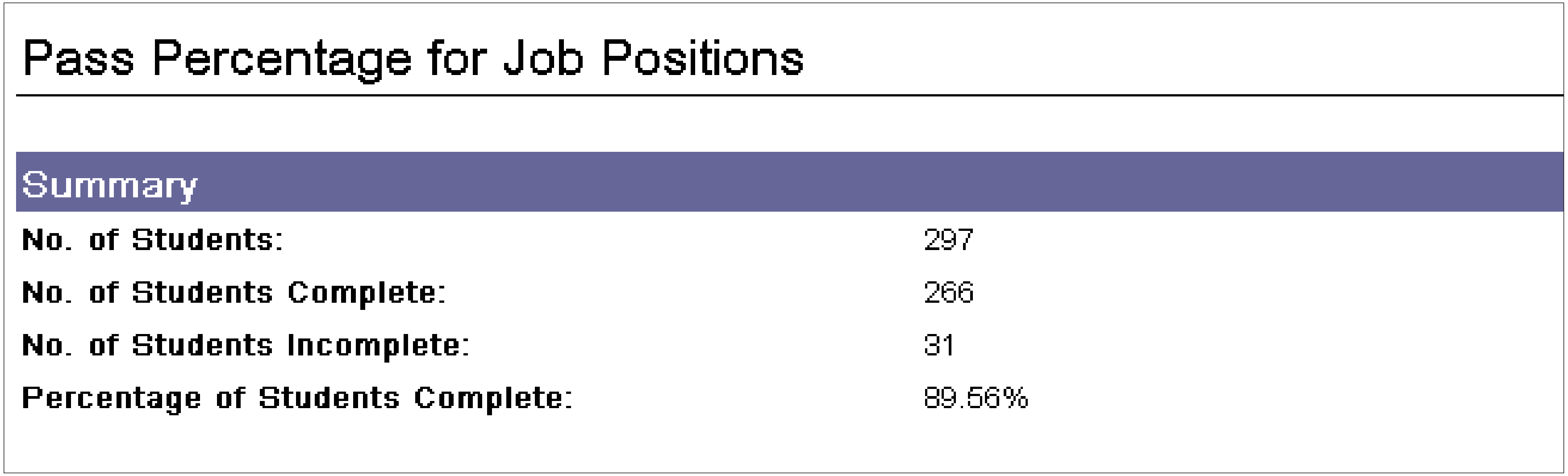
Tools for Compliance

- TMA has provided 3 centrally funded and managed tools to facilitate compliance efforts across the MHS
  - Training Tool
    - Plateau’s Learning Management System (**LMS**)
    - Quick Compliance Course Content
  - Compliance Tool
    - Strategic Management Systems, Inc **HIPAA BASICS** TM
  - PHI Management Tool (**PHIMT**)
    - HIPAA Accelerator’s disclosure tracking tool

Compliance Assurance

Learning Management System (LMS)

- Web based training application that uses online courses to provide and track HIPAA training
- Enterprise solution that supports compliance reporting
  - HIPAA Privacy and Security training compliance status



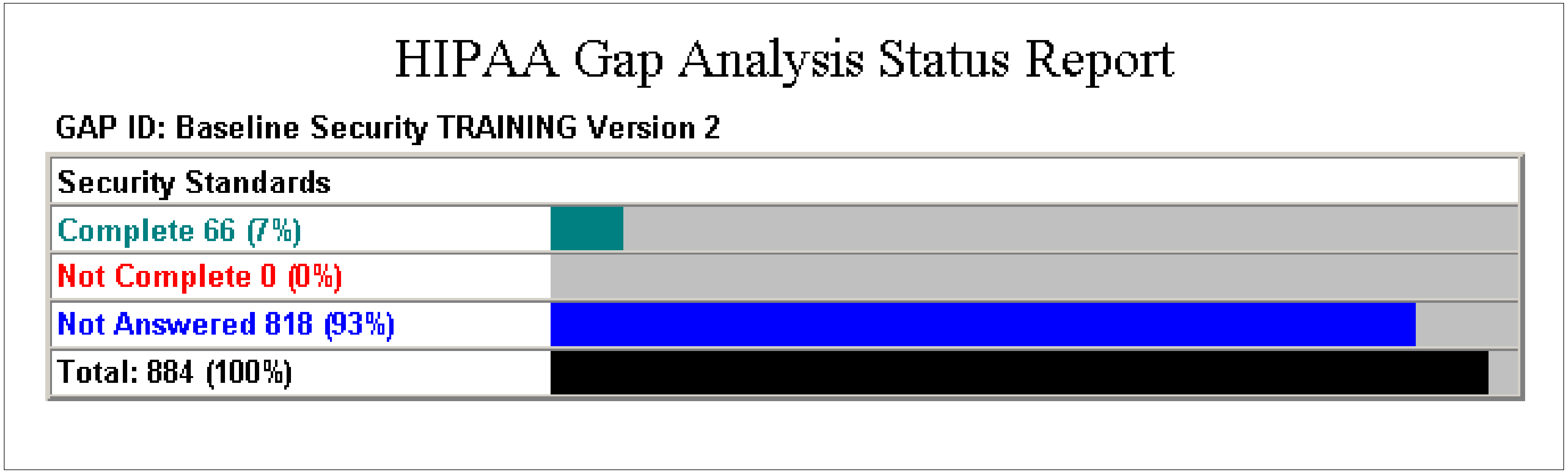
Pass Percentage for Job Positions

Summary	
No. of Students:	297
No. of Students Complete:	266
No. of Students Incomplete:	31
Percentage of Students Complete:	89.56%

Compliance Assurance

HIPAA BASICS

- Web based application that allows users to conduct compliance assessments based on the HIPAA Privacy and Security regulations
- Users can track their level of compliance with the use of reports and project plans based on their assessments



HIPAA Gap Analysis Status Report

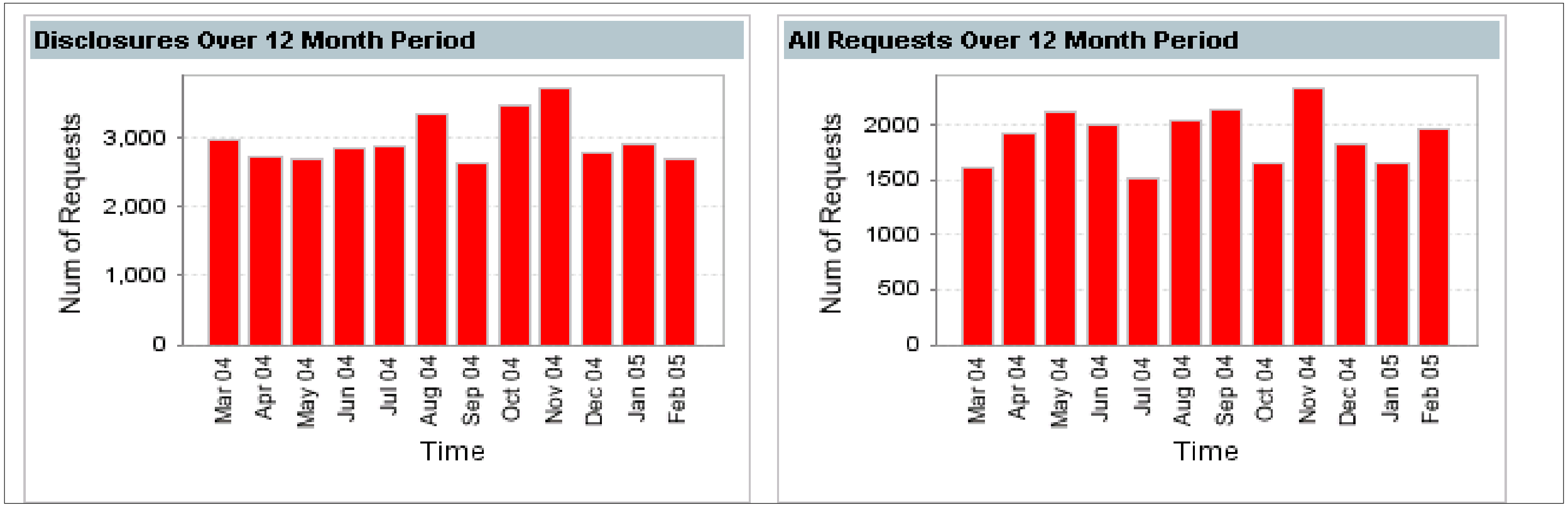
GAP ID: Baseline Security TRAINING Version 2

Security Standards
Complete 66 (7%)
Not Complete 0 (0%)
Not Answered 818 (93%)
Total: 884 (100%)

Compliance Assurance

Protected Health Information Management Tool (PHIMT)

- Web based application used to assist in complying with the HIPAA Privacy disclosure accounting requirement
- Allows users to track disclosures, document complaints, requests for amendments and authorizations, and restrictions to PHI
- Administrative summaries provide a high level dashboard for administrators to track disclosure trends over time



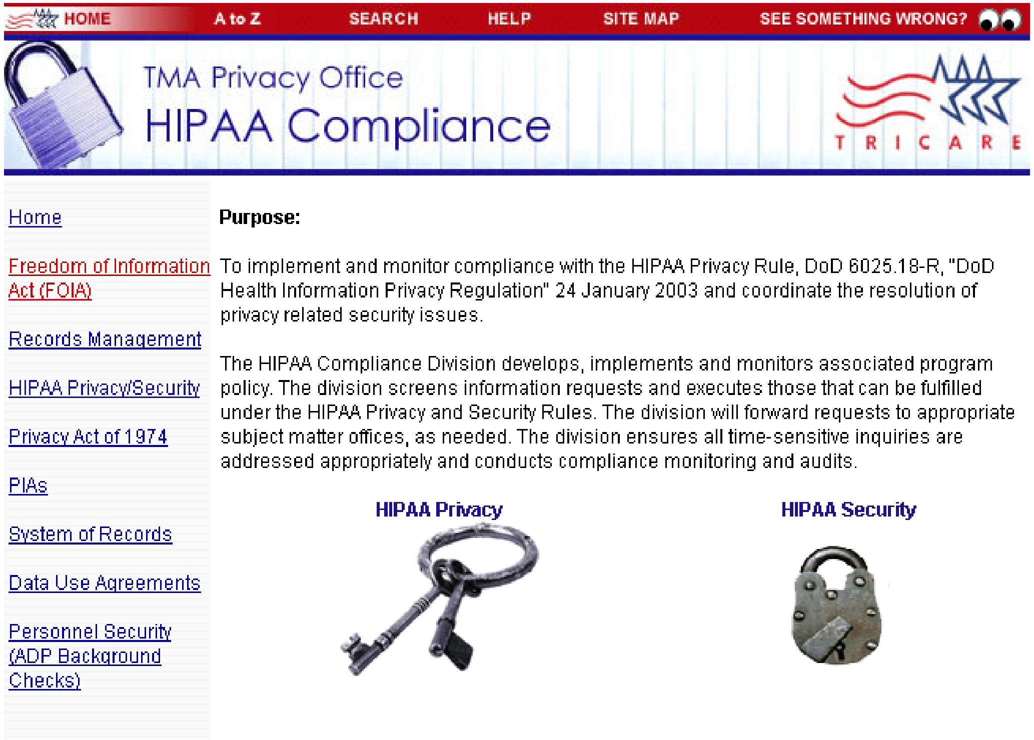
Measuring Compliance

- TMA managed tools:
  - Allows MHS to demonstrate to Health and Human Service, DoD Senior Leadership and our beneficiaries that we care about protecting their information
  - Produce documentation that can verify and validate our processes that ensure those protections
  - Provide a mechanism for capturing workload to demonstrate level of effort to achieve and maintain HIPAA compliance

Compliance Assurance

Resources (1 of 2)

- TMA has provided multiple resources to facilitate compliance
  - Website
  - Information and guidance papers
  - Policies



Purpose:

To implement and monitor compliance with the HIPAA Privacy Rule, DoD 6025.18-R, "DoD Health Information Privacy Regulation" 24 January 2003 and coordinate the resolution of privacy related security issues.

The HIPAA Compliance Division develops, implements and monitors associated program policy. The division screens information requests and executes those that can be fulfilled under the HIPAA Privacy and Security Rules. The division will forward requests to appropriate subject matter offices, as needed. The division ensures all time-sensitive inquiries are addressed appropriately and conducts compliance monitoring and audits.

Compliance Assurance

Resources (2 of 2)

- TMA has provided funding for FY 2002 – 2005
  - Services were asked in FY 2003 to POM for HIPAA Resources beginning in FY 2006
  - Resources to date have funded:
    - Training Conferences
    - Travel funds for Training Conference attendance
    - HIPAA Support Contracts for each Service
      - Headquarter Level
      - Regional/MTF support personnel

Corbis.com

Compliance Assurance

Summary

- You should now be able to:
  - List methodologies for Compliance Assurance
  - Describe proposed reporting requirements for HIPAA compliance
  - List the tools and resources available for oversight activities

Summary

- You should now be able to:
  - Describe the reasons for Oversight
  - List methodologies for Compliance Assurance

Resources

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003
- HIPAA Security Rule
- http://www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- HIPAA privacy and security service representatives